View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Digital library of Brno University of Technology

A Chaotic IP Watermarking in Physical Layout Level Based on FPGA

Wei LIANG[1, 2], *[*]Xingming SUN*[1], *Zhihua XIA*[1], *Decai SUN*[1], *Jing LONG*[2]

[1]School of Computer and Communication, Hunan University, Changsha, 410082, China
[2]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China

idlink@163.com, sunnudt@163.com, xia_zhihua@163.com, sdecai@163.com, longjing0404@163.com

[*]Corresponding author: *Xingming SUN*, tel.: 86-731-88821341; fax: 86-731-88821341

Abstract. *A new chaotic map based IP (Intellectual Property) watermarking scheme at physical design level is presented. An encrypted watermark is embedded into the physical layout of a circuit by configuring LUT (Lookup Table) as specific functions when it is placed and routed onto the FPGA (Field-Programmable Gate Array). The main contribution is the use of multiple chaotic maps in the processes of watermark design and embedding, which efficiently improves the security of watermark. A hashed chaotic sequence is used to scramble the watermark. Secondly, two pseudo-random sequences are generated by using chaotic maps. One is used to determine unused LUT locations, and the other divides the watermark into groups. The watermark identifies original owner and is difficult to detect. This scheme was tested on a Xilinx Virtex XCV600-6bg432 FPGA. The experimental results show that our method has low impact on functionality, short path delay and high robustness in comparison with other methods.*

Keywords

IP reuse technology, FPGA, chaotic map, LUT, IP watermarking.

1. Introduction

With the rapid development of deep sub-micron integrated circuit systems, people expect that more logic functions could be integrated into one piece of silicon. Gradually, Field Programmable Gate Array (FPGA) has emerged and become a mainstream technology in IC design. Meanwhile, in most of FPGA-based designs [1], [2], intellectual property (IP) reuse technology is widely used for shortening design cycle and reducing product risk. Therefore, the problem of effective IP protection has been concerned by more and more semiconductor companies.

Recently, digital watermarking has evolved as a mature technology to protect the authorship of multimedia source of text, image and video [3-5]. Many researchers have attempted to solve IP protection problem existed in deep sub-micron IC systems [4-7, 11-27] on the basis of digital watermarking. IP watermarking has emerged as a novel technology for IP protection, which provides convincing evidence by hiding ownership information in designs. The reuse-based design flow is stated as follows. Firstly, the design specification and structure are determined according to the actual needs. The system level model should also be built. Then we describe and simulate the behavior of the design. The physical layout is generated after that. Finally, we generate the bitfile and download to the target device for verification [4], [5]. The outputs in various levels are collectively called IP modules, which can be used in other design. Reusable IP cores are classified into three categories: soft IP, firm IP and hard IP [6], [7], as shown in Fig. 1.

IP watermark can be embedded at various levels in design flow, which are system level, behavioral level, structural and physical level from high to low. The watermark can only be detected at the embedded level or lower levels. The watermarked IP has low probability of coincidence. Thus IP protection problem has been solved. Considering the criteria of multimedia watermarking [3] and features of IP cores, IP watermarking should have the following characteristics:

- Robustness. Watermark can survive various regular manipulation or attacks and can be extracted correctly.
- Reliability. After embedding watermark, IP core becomes a unique design with low probability of coincidence, thus provide convincing evidence to prove the identity of the IP circuit.
- Transparency. Embedding watermark has no impact on design function and is not easily found.
- Low overhead. The overhead of watermark embedding and extraction is much lower than that of the original design.
- Good traceability. Embedding watermark at a design level, watermark can be traced at lower levels even after IP has been packaged.
- Low impact on performance. The performance in terms of area, power and speed should not be degraded obviously after embedding watermark.

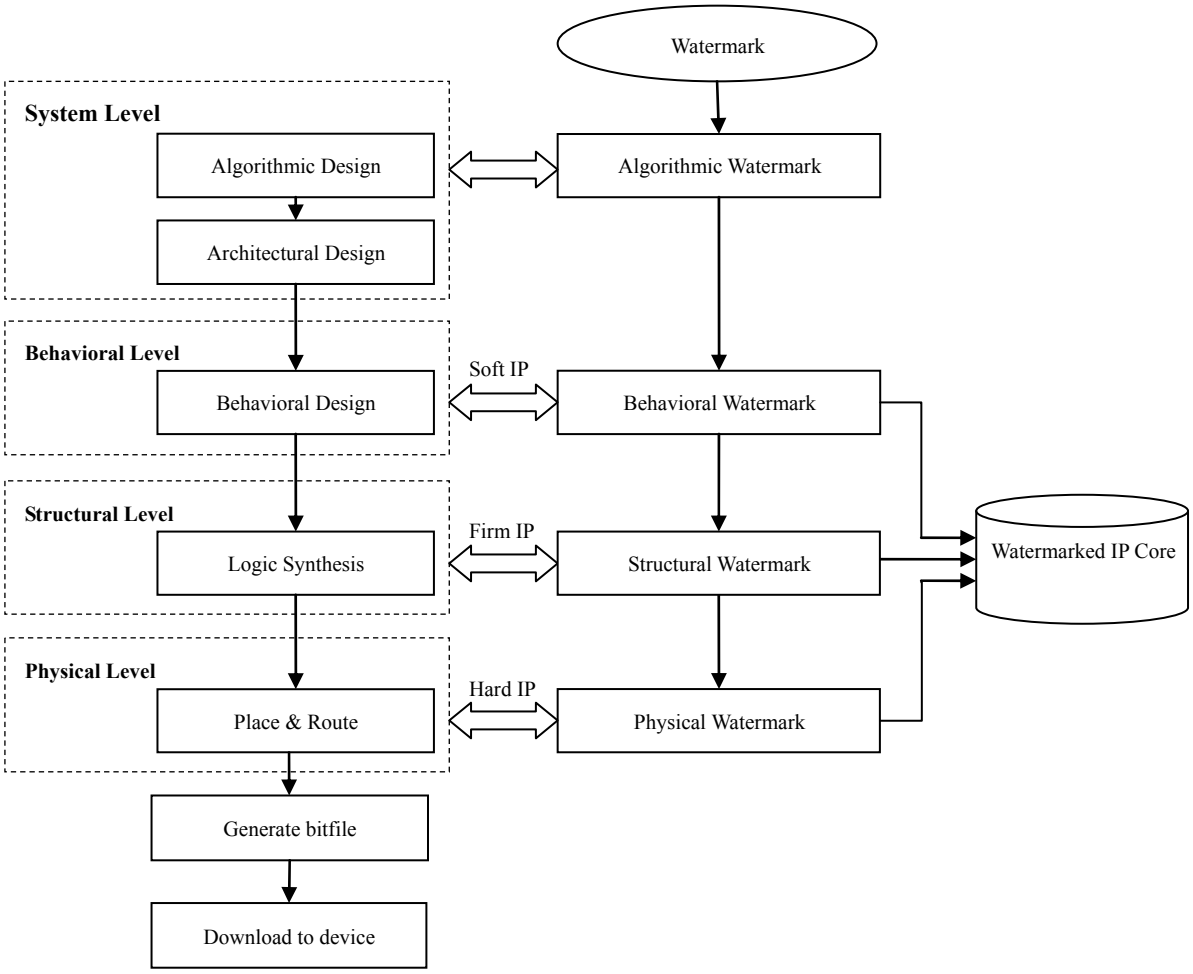


Fig. 1. Flow chart of IP design and watermark at different levels.

The rest of the paper is organized as follows: Section 2 discusses previous approaches to IP watermarking. Section 3 introduces relevant definitions about chaotic map, builds watermarking mathematic model and describes the processes of watermark embedding and extraction in details. Section 4 presents experimental results and analyzes the performance of the proposed method and the paper is summarized in section 5.

2. Related Work

Chaotic map is a determinate and random process in nonlinear dynamical system, which is non-periodic, non-convergent and depending on initial value sensitively [8-10]. Chaos-based security technology is widely used in the fields of network security, secure communication and copyright protection. In the application of IP protection, chaotic sequences are generated randomly and sensitive to initial value, which is consistent with the security and randomness of watermark in IP reuse.

IP protection in reuse-based design is mainly post-processing based on FPGA [11-15]. Early in the 1990s, Lach et al. [16-18] first proposed the concept of FPGA-base watermarking and conducted lots of studies on this field. The methods in [16-18] encrypt the signature of IP owner, and embed it in unused LUT of FPGA. Inputs of these LUTs are taken from passing signals and outputs are routed to neighboring "don't care" inputs, then they are incorporated into the design. Kahng et al. [19] proposed the constraint-based IP watermarking. The method encodes the signature into an optimization problem and generates a unique watermarked design by limiting the solutions space to a certain area. Castillo et al. [20], [21] presented a method for embedding watermark at hardware description language (HDL) level. The watermark is inserted into unused LUTs or between used LUTs in FPGA-based design. The hardware overhead is primarily caused by watermark extraction circuit. Once the watermark extraction circuit detects a specific input sequence, the watermark will orderly be output from the store address. In the constraints based watermarking scheme proposed by Qu et al. [23], the watermark is divided into two parts: public and private. The public watermark can be detected in public and the third party is responsible for IP identification, while private watermark can only be detected by several authorized users to solve the difficulties in IP detection and authorization. A. K. Jain et al. [24] presented a zero overhead FPGA watermarking method by modifying time constraints of the nets for watermark embedding. Furthermore, Fingerprinting

techniques for FPGA IP protection have been proposed in [16], [25], this approach obtains fingerprints of different users, then embeds this fingerprint information in IP circuit. These approaches are of great use for IP protection and infringement tracking. However, the power overhead and path delay are accordingly increased.

Most constraint-based watermarking scheme have been proposed at physical design level [11-19], [23-26], while less at structural level and behavioral level [5], [20-22]. By using these methods, it is hard for unauthorized users to detect, remove or modify the watermark. Therefore, the security of watermark will be improved. However, the performance in terms of power, area and circuit delay may be partly affected.

A chaotic map based IP watermarking scheme is proposed by considering less interference with normal function, minimum path delay and high security. In the scheme, we design a special structure for inserting watermark into LUT. The structure determines the locations of unused LUTs for watermark insertion. The watermark bits are controlled by the generated random sequences. The experimental results show that the proposed scheme has low impact on performance and the amount of embedded watermark has been greatly increased. Therefore, convincing evidence has been provided to prove the identity of original ownership.

3. Chaotic Watermark Algorithm

3.1 Chaotic Model

Chaotic map is introduced to improve the security of IP watermark. This section first gives relevant definitions and then introduces a new watermarking mathematic model.

Definition 1: Chaotic behavior of Logistic map can be represented by one-dimensional non-linear function [19], [20], that is:

$$x_{n+1} = \lambda x_n (1 - x_n), \quad \lambda \in (0,4), x_n \in (0,1), n = 0,1,\cdots \tag{1}$$

In (1), Logistic map is in chaos when $\lambda \in (3.5699456, 4)$. That is, given initial value X_0, the sequence $\{x_i \mid i = 0, 1, \ldots, N\}$, generated by Logistic map is non-periodic, non-convergent and depending on initial value sensitively, called chaotic sequence. Transform the real chaotic sequence generated by (1) into {0,1} binary chaotic sequence, and then take m bits of the binary chaotic sequence orderly to form a decimal chaotic sequence $\{d_i \mid 0 < d_i < 2^m, i = 0, 1, 2, \ldots\}$, represented by C.

Definition 2: To avoid collision in chaotic scrambling, we hash sequence C using static hash table, and hash chaotic sequence F is generated.

Select two initial values X_0, X_1 and X_2, and use definition 1 and 2 for the generation of hash chaotic sequence F_l, F_c and F_s:

$$F_l = \{l_1, l_2, \cdots l_N\}, \tag{2}$$

$$F_c = \{c_1, c_2, \cdots, c_N\}, \tag{3}$$

$$F_s = \{s_1, s_2, \cdots, s_N\}. \tag{4}$$

3.2 Principle of LUT Watermark Embedding

FPGA architecture mainly consists of configurable Logic Block (CLB), input/output block (IOB) and block RAM. As a basic assumption, all of the discussion and experimental work are in the context of the Xilinx XCV600 architecture, where CLBs each contains two flip flops (FF) and two 16×1 lookup tables (LUT).

Most of FPGA-based designs will contain large number of unused LUTs. Each n-input LUT could be regarded as a $2^n \times 1$ RAM and one bit in unused LUT can be used to encode one bit watermark. In this case, a 4-input LUT can encode 16 bits watermark at most. Arbitrary combinational logic with n variables could be implemented in n-input LUT. Considering that, we propose to embed watermark by configuring unused LUTs in FPGA design. The development platform Xilinx ISE 9.1i is used in the proposed method. The signature is encoded into specific combinational logics by using code rules. The combinational logics are then implemented in selected unused LUTs, with the outputs as the watermark. Here, we use chaotic map for better security of watermark.

Fig. 2 shows an example of configuring a specific function for indicating watermark. The signature

F=(A1 and A2) or (A3 xor A4)						
input	A1	0	0	0	…	1
	A2	0	0	0	…	1
	A3	0	0	1	…	1
	A4	0	1	0	…	1
output	O	0	1	1	…	1

watermark

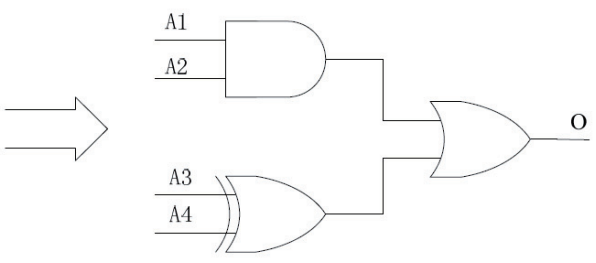


Fig. 2. Example of implementing a F= (A1 and A2) or (A3 xor A4) function for watermark indication.

"hnulw…" is encoded into ASCII code and then scrambled as watermark "011…1". The scrambled watermark is divided into a number of watermark fragments by using chaotic sequence F_c. With the sequence F_l, the locations for embedding watermark are determined. By using FPGA editor tool, the fragments are inserted into the unused LUTs by configuring the unused LUTs at these locations. With the watermark fragment, the function F = (A1 and A2) or (A3 xor A4) could be implemented by configuring the unused LUT. Finally, the watermarked LUTs will be incorporated into the design with some "don't care" interconnects. It is hard for the attackers to detect the locations of watermarked LUTs. Thus the security and reliability of watermark are greatly improved.

3.3 Embedding and Extraction of Chaotic Map IP Watermark

Two sequences are generated respectively for determining the locations of unused LUTs and controlling the embedded watermark bits. Since chaotic map depends on initial value and is sensitive to parameters, we propose to embed watermark in unused LUT randomly. As a result, the strength of watermark is enhanced.

3.3.1 Watermark Embedding

The flow chart of watermark embedding is shown in Fig. 3. Supposing the ownership information is "hnulw…",

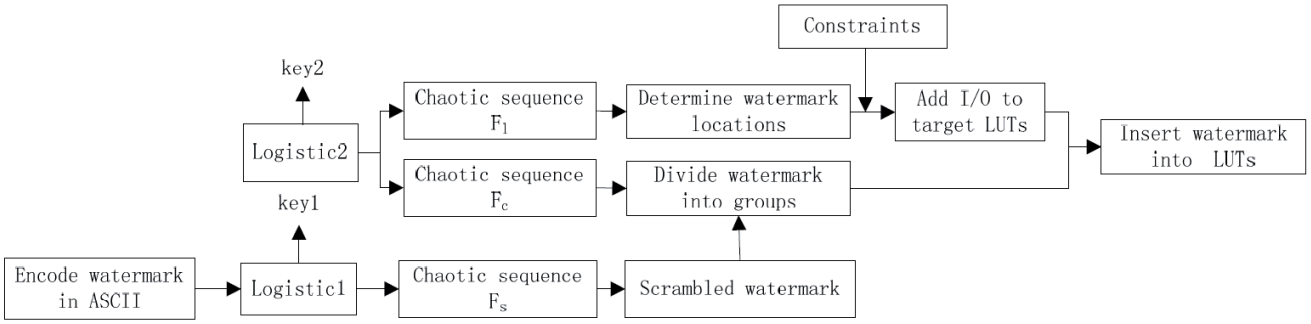


Fig. 3. Flow chart of watermark embedding.

the embedding process is stated as follows:

Input: Original ownership information W, the carrier (IP core)

Output: watermarked carrier

Step 1: The ownership information W is encoded into ASCII code, indicating the watermark. Then we generate a hash chaotic sequence F_s, denoted by $s_1, s_2,\ldots,s_N$,(*key1* as the key) for scrambling the watermark. Finally the scrambled watermark is generated for embedding;

Step 2: Add a set of additional constraints to make the locations of watermarked LUT close to used LUTs. The constraints are programmed in user constraints file of ISE tool. In this case, overlong nets between LUTs will not emerge in the watermarked design. Meanwhile, the resource occupation and path delay will not increase obviously;

Step 3: Given two initial values (*key2* as the key), two hash chaotic sequences F_l and F_c are generated for determining locations of unused LUTs p_i $(1 < i < N)$ and controlling embedded watermark bits g_i $(1 < i < N)$;

Step 4: The scrambled watermark sequence is divided into groups $g = \{g_1, g_2,\ldots,g_N\}$ by using chaotic sequence F_c;

Step 5: According to the locations for embedding watermark $p = \{p_1, p_2,\ldots,p_N\}$ and embedded watermark bits $g = \{g_1, g_2,\ldots,g_N\}$, we build the logic functions $f = f_1, f_2,\ldots,f_N$, with the outputs indicating watermark;

Step 6: Since an arbitrary combinational logic with 4 variables could be implemented in a 4-input LUT, we implement various functions f in multiple unused LUTs for embedding watermark fragments. After all the functions are configured, the watermarked IP is generated.

3.3.2 Watermark Extraction

When the IP core is suspicious to be misappropriation, the author could apply to the third party for the verification

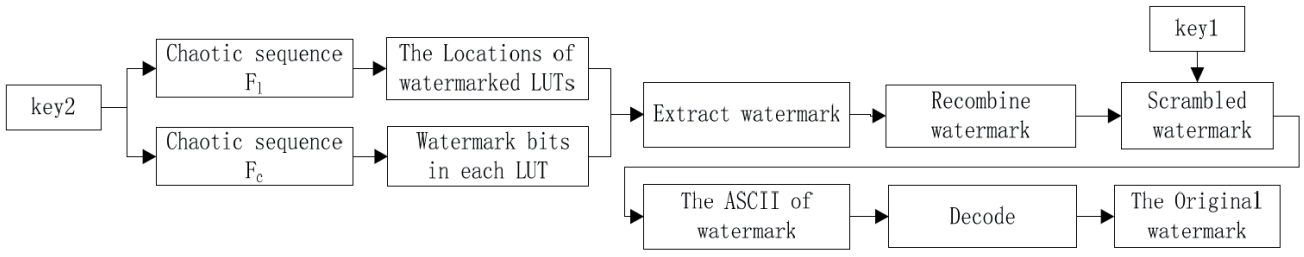


Fig. 4. Flow chart of watermark extraction.

of watermark. The IP owner provides the reversed sequences and signature that they used in watermark embedding. With the signature and the sequences, the unbiased validation team reverses the watermark preparation and embedding process: identify the LUTs used for embedding watermark using the sequence F_l, extract the logic outputs at these locations, combine and decrypt the message to print out the resulting signature. If the signature matches that provided by the IP owner, then ownership has been established. The flow chart of watermark extraction is shown in Fig. 4; the detailed steps are as follows:

Input: Initial chaotic keys: *key1*, *key2* and the carrier (IP core)

Output: The original ownership information W

Step 1: Establish mapping relations between watermarked carrier and elements of scrambled watermark sequence $\{S_i, 1 \le i \le N\}$;

Step 2: Obtain chaotic sequences F_l and F_c with *key2* and extract the logic function $f = f_1, f_2, \ldots, f_N$, implemented in LUT;

Step 3: Restore the function in step2 and obtain the watermark groups embedded in LUT $g = \{g_1, g_2, \ldots, g_N\}$;

Step 4: Extract watermark groups embedded in the locations $p = \{p_1, p_2, \ldots, p_N\}$ and recombine the groups as ASCII code of original watermark W;

Step 5: Decode the ASCII code of watermark and get the original ownership information W.

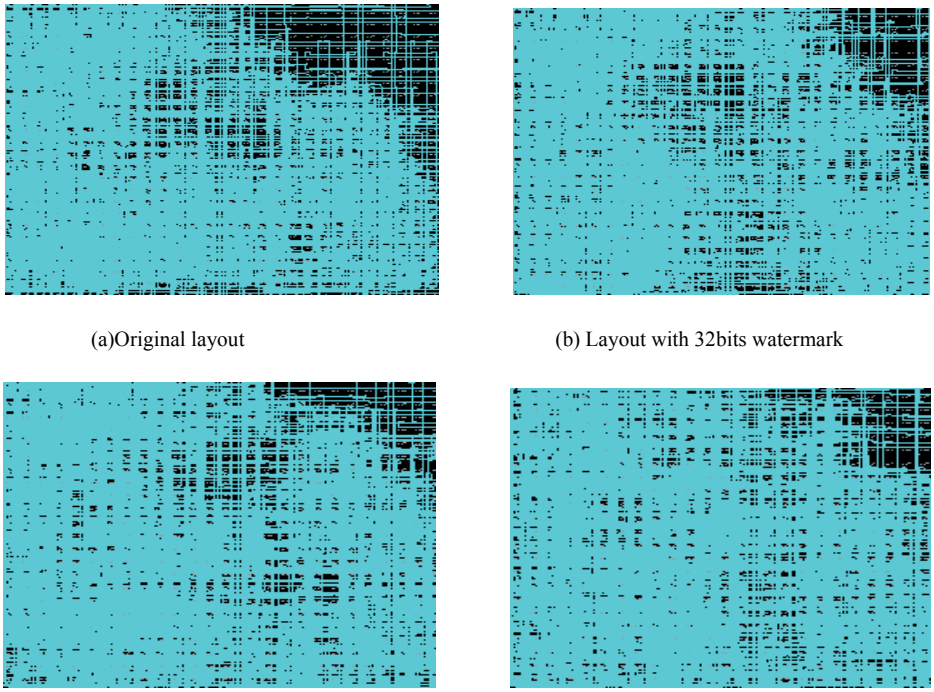
4. Experiments and Performance Analysis

4.1 Experiments

We verified the method in the context of Xilinx Virtex XCV600-6bg432, with operating frequency 75.3 MHz and IP cores: DES56 [27], MD5 [28], RSA [29]. This section gives the physical layouts of IP core before and after embedding watermark.

Take DES core for example, first of all, we perform compiling, synthesis, place and route on DES core; in the end we obtain the original layout of DES in Fig. 5 (a). Using our method respectively embeds watermark of 32 bits, 256 bits and 512 bits, the watermarked layouts are presented in Fig. 5(b), Fig. 5(c) and Fig. 5(d). As seen in Fig. 5(a-d): the physical layout in Fig. 5(b) with 32 bits watermark has denser nets and larger area than the original layout in Fig. 5(a), the area of the results in Fig. 5(c) and Fig. 5(d) increase to some extent. It can be concluded that the overall physical layout of IP core will be changed by using our method for embedding watermark, but without interfering with robustness and security of the circuit, and stable performance of the circuit can be achieved at the cost of area.

In addition, we compare our method with methods in [6] and [11]. The experimental results are presented in Table 1. The occupied resource and delay time are respec-



(a)Original layout (b) Layout with 32bits watermark

(c)Layout with 256bits watermark (d) Layout with 512bits watermark

Fig. 5. Physical layout of DES (original, 32bits watermark, 256bits watermark and 512bits watermark).

Core	Watermarking Method	32bit W.M		256bit W.M		512bit W.M	
		%resources	%time	%resources	%time	%resources	%time
DES	Literature[6]	0.325	0.162	1.836	-0.171	3.461	-2.312
	Literature [11]	0.413	-0.087	1.761	-0.129	3.823	-3.165
	Ours	0.487	-0.102	1.939	-0.273	4.079	-3.986
RSA	Literature [6]	0.478	0.092	2.655	0.231	4.572	2.341
	Literature [11]	0.568	0.077	2.732	-0.635	5.231	-3.562
	Ours	0.575	0.089	2.744	-0.804	5.776	-3.707
MD5	Literature [6]	0.279	0.166	1.685	1.021	3.127	-0.011
	Literature [11]	0.354	-0.146	1.852	-1.219	3.408	-1.188
	Ours	0.373	-0.255	2.074	-1.276	3.842	-2.170

Tab. 1. Performance comparison with different methods based on DES, RSA, MD5.

tively shown after embedding 32bit, 256bit and 512bit watermark. We conclude that the occupied resource will be a bit higher than other methods, while the delay time will decrease with the increase of embedded watermark.

4.2 Resistance to Attacks

Resistance to attacks is the ability of watermark being extracted correctly after various unauthorized attacks. For general FPGA-based IP watermarking, it is hard for attackers to extract original watermark. However, the attackers may obtain the key of watermarked locations by power attack and destroy the watermark. Power Attack [30], [31] is actually an effective key attack, which could guess the key by analyzing the power of cipher module. Multi-thread power analog technology [32] is used to quantify the resistance of cipher component to power attack in IP design and implementation.

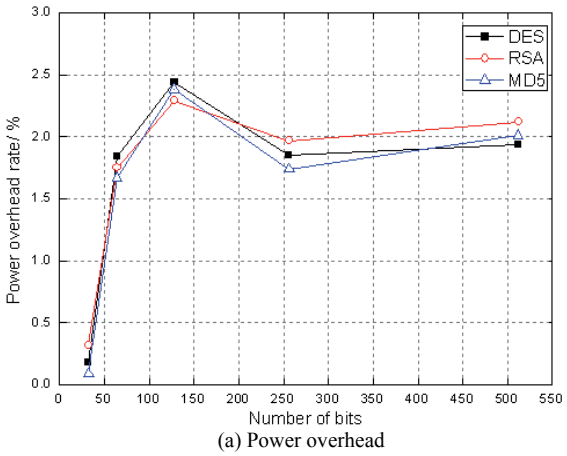
Therefore, multi-thread power analog technology is adopted to quantify the resistance to Power Attack of the watermarked components, meanwhile, some "don't care" nets are connected with the watermarked LUTs, thus the function and performance will not be interfered, and the ability of resistance to Power Attack can be improved.

4.3 Detection

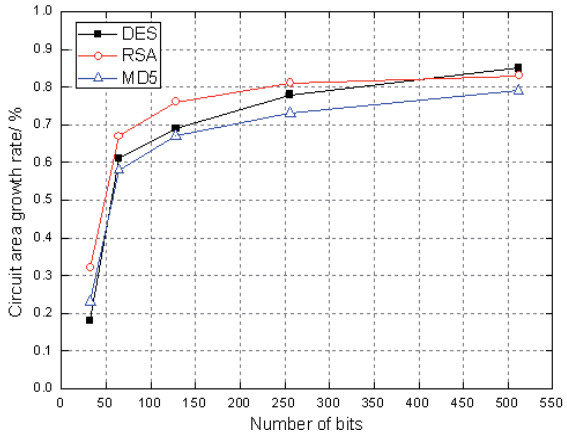
By using the approach in this paper, with the chaotic key *key2* we can get two chaotic sequences F_l and F_c, from which we know the embedding locations and watermark bits in unused LUTs of FPGA, then with *key 1* for restoring the original watermark, and finally prove the identification of the ownership.

4.4 Circuit Area and Power Consumption

Circuit area and power consumption of IP core mainly refers to the extra area and power overhead in the process of watermark embedding. Fig. 6 shows the trend of area and power of three testing cores with the increase of watermark. Fig. 6(a) shows an ascendant trend of power consumption with the increase of embedded watermark, but a downtrend of the increase rate. It is caused by that occupation of CLB



(a) Power overhead



(b) Circuit area

Fig. 6. Growth curves of power overhead and circuit area with the increase of embedded watermark.

increases rapidly in the embedding prophase, while the embedding of anaphase is on the basis of CLB occupied in prophase. Therefore, the nets within CLB grow with the increase of embedded watermark, while nets outside CLB may decrease, this may affect the rate of power consumption to a certain extent. As shown in Fig. 6(b), with the increasing amount of embedded watermark, the circuit area overhead continuously grows overall, but the circuit area grows rapidly in the embedding of 256bits watermark, after that, the increasing watermark causes a flat trend of the area growth.

5. Conclusions

In this paper, a chaotic map-based IP watermarking at physical level is presented for IP protection in reuse technology. This approach uses multiple chaotic sequences in watermark embedding, thus improves security of IP watermark and verifies the circuit functions before and after watermarking using Modelsim6.2SE. The performance was verified in the context of Virtex XCV600-6bg432. The experimental results show that our approach has low impact on the normal function. Though the circuit area increases after embedding watermark, the performance in terms of path delay, robustness and security are guaranteed. Future work may focus on IP watermarking method at various levels, which includes optimization of watermarking method at high levels, adding testing circuit and implementation of equivalent circuit with resistance to attack.

Acknowledgments

This work is supported by National Basic Research Program of China (973 Program) under Grant No. 2009CB326202 and 2010CB334706. Key Program of National Natural Science Foundation of China under Grant No. 60736016. National Natural Science Foundation of China under Grant No. 60873198, 60973128, 61073191, 61070196 and 60973113. Scientific Research Fund of Hunan Provincial Education Department under Grant No. 09C403, National Natural Science Foundation of Hunan Province and Xiangtan united Foundation under Grant No. 09JJ9006, Key Program of Scientific Research Fund of Hunan Provincial Education Department under Grant No. 09A027.

References

[1] CHANG, H., COOK, L., et al. *Surviving the SOC Revolution: A Guide to Platform-Based Design.* Norwel, MA: Kluwer Academic Publishers, 1999.

[2] MARTIN, G., CHANG, H. *Winning the SoC Revolution: Experiences in Real Design.* Norwell, MA: Kluwer Academic Publishers, 2003.

[3] COX, I. J., MILLER, M.L., BLOOM, J.A. *Digital Watermarking.* New York: Morgan Kaufmann Publishers, 2002.

[4] ABDEL-HAMID, A. T., et al. IP watermarking techniques: survey and comparison. In *Proc. of the 3rd IEEE International Workshop on System-on-Chip for Real-Time Applications.* 2003, p. 60-65.

[5] FAN, Y. Testing-based watermarking techniques for intellectual-property identification in SOC design. *IEEE Trans. on Instrumentation and Measurement,* 2008, vol. 57, no. 3, p. 467-479.

[6] SCHMID, M., et al. Netlist-level IP protection by watermarking for LUT-based FPGAs. In *Proc. of IEEE International Conference on Field-Programmable Technology,* 2008, p. 209-216.

[7] KHAN, M., TRAGOUDAS, S. Rewiring for watermarking digital circuit netlists. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2005, vol. 24, no. 7, p. 1132-1137.

[8] WANG, H., HE, C., DING, K. Robust public watermarking based on chaotic map. *Journal of Software,* 2004, vol. 15, no. 8, p. 1245-1251.

[9] MUNIR, R., et al. Secure spread spectrum watermarking algorithm based on chaotic map for still images. In *Proc. of the International Conference on Electrical Engineering and Informatics,* 2007, p. 180-183.

[10] ZHANG, C., ZHANG, J. Robust image watermarking based on chaotic mapping. *Acta Electronica Sinica,* 2002, vol. 30, no. 1, p. 69-72.

[11] NI, M., GAO, Z. Constraint-based watermarking technique for hard IP core protection in physical layout design level. In *Proc. of IEEE 7th Int. Conf. on Solid-State and Integrated Circuits Technology,* 2004, p. 1360-1363.

[12] SAHA, D., et al. Fast robust intellectual property protection for VLSI physical design. In *Proc. of IEEE 10th Int. Conf. on Information Technology,* 2007, p. 1-6.

[13] SAHA, D., et al. A novel scheme for encoding and watermark embedding in VLSI physical design for IP protection. In *Proc. of the Int. Conf. on Computing: Theory and Applications,* 2007.

[14] NIE, T., et al. A post layout watermarking method for IP protection. In *Proc. of IEEE Int. Symposium on Circuits and Systems,* 2005, p. 6206-6209.

[15] NEWBOULD, R. D., et al. A hierarchy of physical design watermarking schemes for intellectual property protection of IC designs. In *Proc. of IEEE Int. Symp. on Circuits and Systems,* 2002, vol. 4, p.862-865.

[16] LACH, J., MANGIONE-SMITH, W. H., POTKONJAK, M. Signature hiding techniques for FPGA intellectual property protection. In *IEEE/ACM Int. Conf. on Computer-Aided Design,* 1998, p. 186-189.

[17] LACH, J., MANGIONE-SMITH, W. H., POTKONJAK, M. Fingerprinting techniques for field-programmable gate array intellectual property protection. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems,* 2001, vol. 20, no. 10, p. 1253-1261.

[18] LACH, J., MANGIONE-SMITH, W. H., POTKONJAK, M. Robust FPGA intellectual property protection through multiple small watermarks. In *Proc. of AMC 36th Design Automation Conference,* 1999, p. 831-836.

[19] KAHNG, A. B., et al. Constraint-based watermarking techniques for design IP protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2001, vol. 20, no. 10, p. 1236-1252.

[20] CASTILLO, E., et al. IPP watermarking technique for IP core protection on FPL devices. In *Proc. of IEEE 16th Conf. on Field Programmable Logic and Applications,* 2006, p. 487-492.

[21] CASTILLO, E., et al. IPP@HDL: efficient intellectual property protection scheme for IP cores. *IEEE Transactions on VLSI Systems,* 2007, vol. 15, no. 5, p. 578-591.

[22] CUI, A., et al. IP watermarking using incremental technology mapping at logic synthesis level. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2008, vol. 27, no. 29, p. 1565-1570.

[23] QU, G. Publicly detectable watermarking for intellectual property authentication in VLSI design. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2002, vol. 21, no. 11, p. 1363-1368.

[24] JAIN, A. K., et al. Zero overhead watermarking technique for FPGA designs. In *Proceedings of Great Lakes Symposium on VLSI,* 2003, p. 147-152.

[25] CALDWELL, A. E., et al. Effective iterative techniques for fingerprinting design IP. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2004, vol. 23, no. 2, p. 208-215.

[26] DU, Y., et al. IP protection platform based on watermarking technique. In *Proc. of the 2009 10th Int. Symp. on Quality of Electronic Design,* 2009, p. 287-290.

[27] *Basic DES Crypto Core: Overview.* [Online] Cited 2009-6-10. Available at: http://www.opencores.org/projects.cgi/web/basicdes.

[28] *SystemC/Verilog MD5: Overview.* [Online] Cited 2009-6-10. Available at: http://opencores.org/project,systemcmd5.

[29] *Basic RSA Encryption Engine: Overview.* [Online] Cited 2009-6-10. Available at: http://opencores.org/projects.cgi/web/basicrsa.

[30] ALIOTO, M., POLI, M. A general model for differential power analysis attacks to static logic circuits. In *PPISCAS 2008.* Piscataway (NJ), IEEE, 2008, p. 3346-3349.

[31] STANDAERT, F.-X., ÖRS, S. B., QUISQUATER, J.-J., PRENEEL, B. Power analysis attacks against FPGA implementations of the DES. In *Field Programmable Logic and Applications,* August 2004, p. 84-94.

[32] TONG, Y., et al. Quantitative evaluation of the cryptographic blocks resistibility to power analysis attack at different design level. *Journal of Computer Research and Development,* 2009, p. 940-947.

About Authors…

Wei LIANG received his BS in automation from Central South University, China, in 2001, MS in computer science and technology from Hunan University of Science and Technology, China, in 2008, and he is currently pursuing his PhD in computer science and technology at the School of Computer and Communication of Hunan University, China. His current research interests include steganography, steganalysis, real-time embedded systems, intellectual property protection, and field programmable gate arrays.

Xingming SUN (Corresponding author) received his BS in mathematics from Hunan Normal University, China, in 1984, MS in computing science from Dalian University of Science and Technology, China, in 1988, and PhD in computing science from Fudan University, China, in 2001. He is currently a professor in the School of Computer and Communication, Hunan University, China. His research interests include network and information security, digital watermarking, digital forensic, database security, and natural language processing.

Zhihua XIA was born in Changde, Hunan, China, in 1983. He received his BS in Hunan City University, China, in 2006, and is currently pursuing his PhD in computer science and technology at the School of Computer and Communication of Hunan University, China. His research interests include steganography and steganalysis, digital forensic, image processing, and pattern recognition.

Decai SUN received his B.E. in Daqing Petroleum Institute, China, 2002, and his M.E. in Hunan University, China, 2009. He is currently pursuing his PhD in computer application of Hunan University, China. His main research interests are natural language processing, information retrieval, computational biology and pattern recognition.

Jing LONG received her BE in Hunan University of Science and Technology, China, in 2009, and is currently pursuing her M.S. in computer application technology at the School of Computer Science and Engineering, Hunan University of Science and Technology, China. Her research interests include real-time embedded systems, intellectual property protection, field programmable gate arrays, wireless sensor networks.